Ruckus SmartZone Configuration - Customer Guide

Adentro Overview

Adentro provides consumers with an amazing WiFi experience at their favorite spots, while helping to grow local businesses by better engaging and targeting their customers. By offering a branded captive portal for your guest WiFi network, customers are given the ability to opt-in to targeted messaging sent using the Adentro platform.

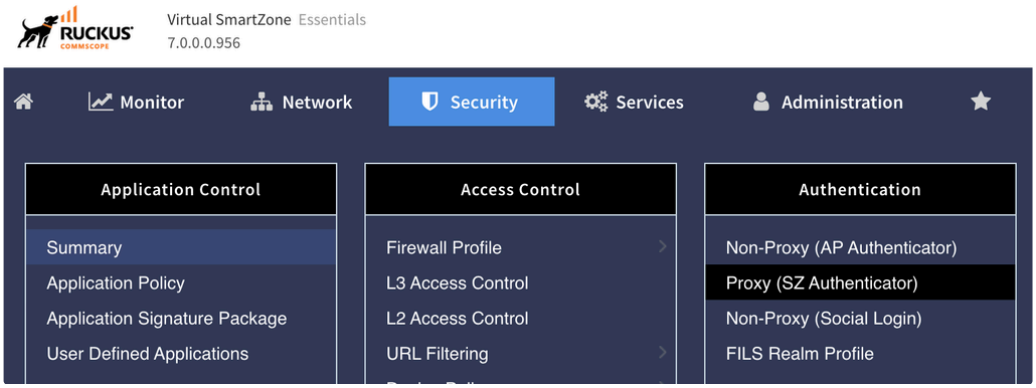
Adentro Configuration

In order to associate your Ruckus access point(s) with your business information, Adentro will need the MAC address of each individual access point that will be broadcasting the integrated SSID. **Please forward your AP MAC address(es) to your Adentro Account Manager.** Without completion of this step, guests will receive a "404" error on the captive portal. **** Disable any other guest networks that are running on other wireless networks to achieve the best results with Adentro ****

Configure AAA

Authentication

1. Under Services and Profiles, select Authentication
2. Select the "Proxy (SZ Authenticator)" tab



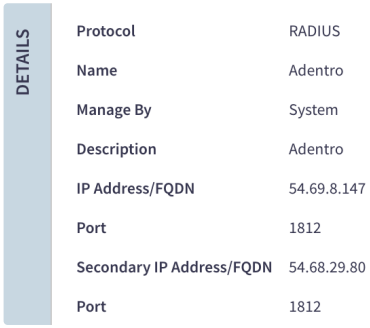
3. Select "Create"
4. Enter the following information:
   Name: Adentro
   Friendly Name: Adentro
   Description: Adentro
   Service Protocol: RADIUS

   Primary Server
   IP Address: 54.69.8.147
   Port: 1812

Secret: 8fc40973252c42e196489d4a16849ff8

Secondary Server
Enable Secondary Server: checked
IP Address: 54.68.29.80
Port: 1812
Secret: 8fc40973252c42e196489d4a16849ff8
Health Check Policy: use default settings

Rate Limiting
Maximum Outstanding Requests: 0
Threshold: 0
Sanity Time: 10s



Accounting

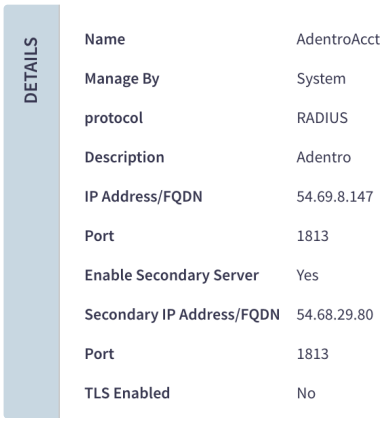
1. Under Services and Profiles, select "Accounting"
2. Select the "Proxy" tab
3. Select "Create"
4. Enter the following information:
   Name: Adentro
   Description: Accounting
   Service Protocol: RADIUS Accounting
   Encryption: TLS Unchecked
   Backup RADIUS: Checked

   Primary Server:
   IP Address: 54.69.8.147
   Port: 1813
   Secret: 8fc40973252c42e196489d4a16849ff8

   Secondary Server:
   Enable Secondary Server
   IP Address: 54.68.29.80
   Port: 1813
   Secret: 8fc40973252c42e196489d4a16849ff8
   Health Check Policy: use default settings

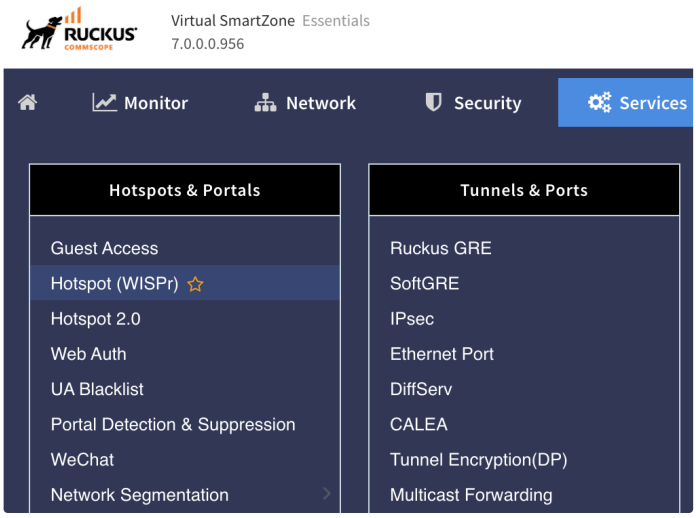
   Rate Limiting
   Maximum Outstanding Requests: 0
   Threshold: 0

Sanity Time: 10s



Configure Hotspot Portal

1. Under Services and Profiles, find the "Hotspots & Portals" section
2. Select the "Hotspot (WISPr)" tab



3. Select "Create"
4. Enter the following information:

   Portal Name: Adentro

   Redirection

   Smart Client Support: None

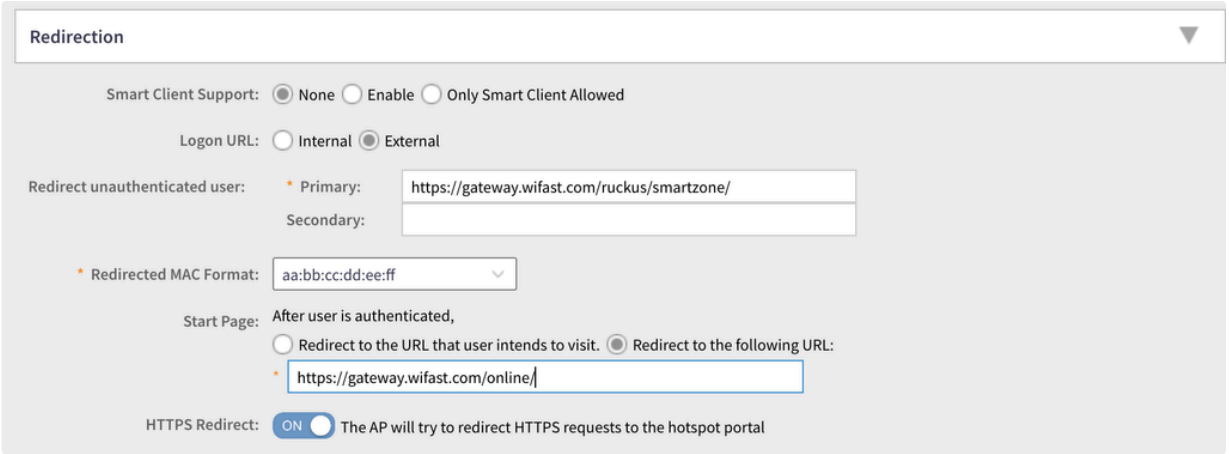
   Logon URL: External

   Redirect URL: https://gateway.wifast.com/ruckus/smartzone/

   Redirected MAC Format: aa:bb:cc:dd:ee:ff

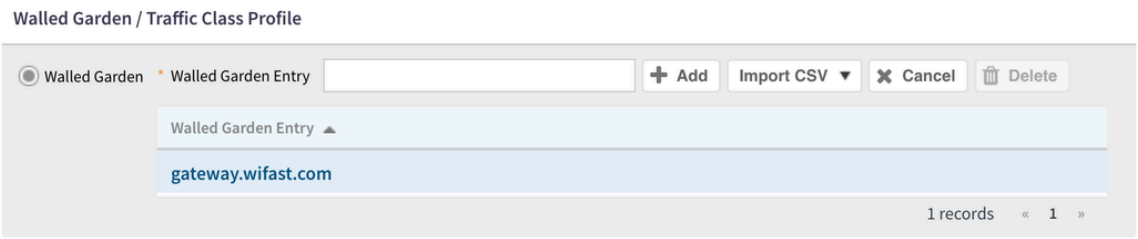
   Start Page: "redirect to the following URL:" https://gateway.wifast.com/online/

   HTTPS Redirect: checked



Walled Garden

gateway.wifast.com



Configure WLAN

1. Under "Wireless LANs", create a new WLAN or edit an existing one
2. Enter the following information:

   Authentication Options

   Authentication Type: Hotspot (WISPr)

   Method: Open

   Encryption Options

   Method: None

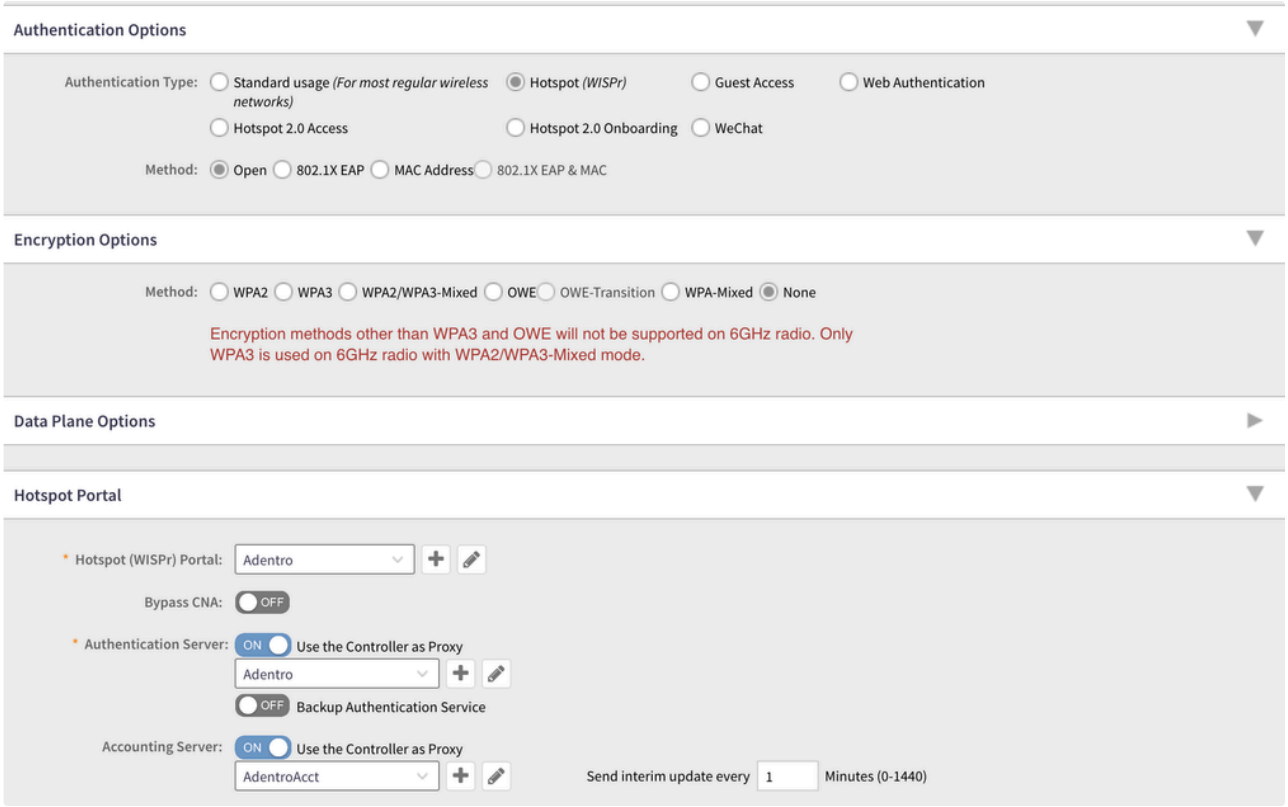
   Hotspot Portal

   Hotspot (WISPr) Portal: Adentro

   Bypass CNA: unchecked

   Authentication Server: check "Use the controller as proxy" and select "Adentro"

   Accounting Server: check "Use the controller as proxy", select "Adentro", and send updates every 1 minute



Wireless Client Isolation

We suggest isolating guest traffic to protect your network and other guests.

Client Isolation: On

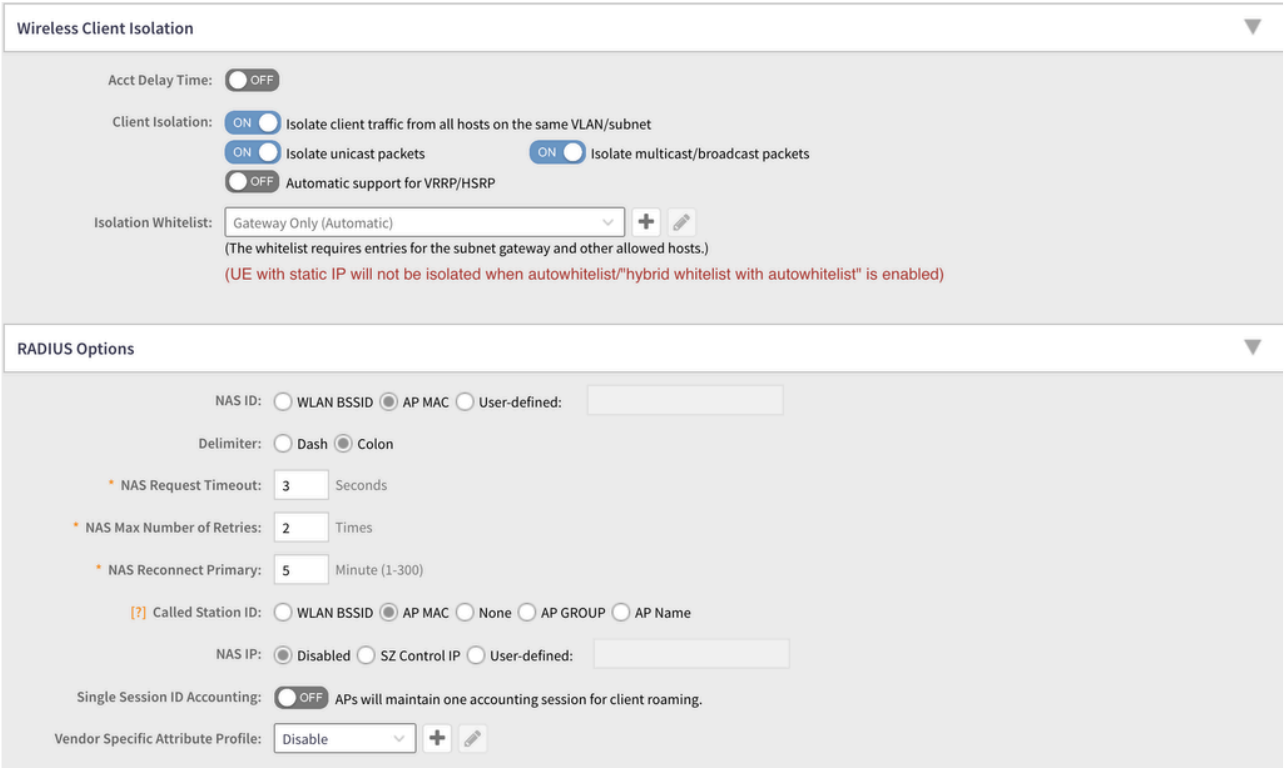
Isolate unicast & multicast packets: On (for both)

RADIUS Options

NAS ID: AP MAC

Delimiter: Colon

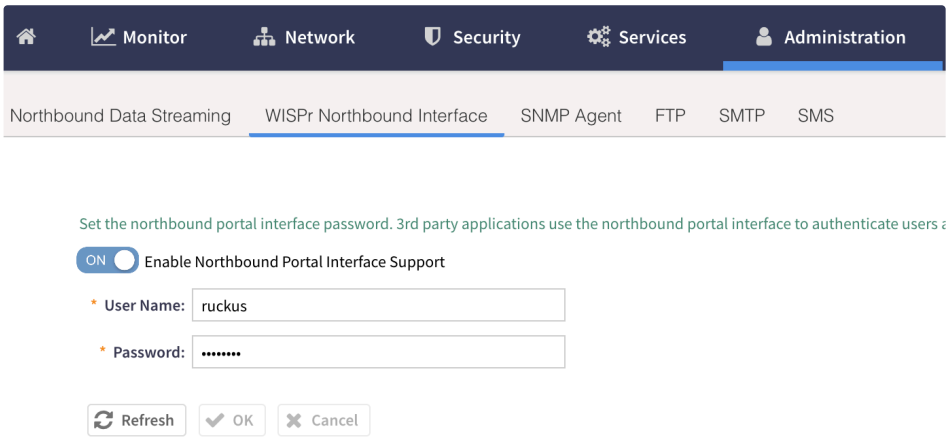
Called Station ID: AP MAC



Configure Northbound Interface

The northbound interface must be configured so that Adentro servers can make requests to decrypt MAC addresses they receive on portal requests. Without this, Adentro cannot determine which location the AP belongs to or which customer the client device belongs to.

1. Under "Administration", select "WISPr Northbound Interface"
2. Check "Enable Northbound Portal Interface Support"
3. Enter username "ruckus" (lowercase "r"), and a secure password.



You will need to ensure the northbound interface is reachable over the internet on a static IP, so that Adentro servers can reach it. It should be available on TCP port 9443. Ensure any firewalls and port forwarding will allow this (See Firewall Rules section below).

To test that the northbound interface is available, you can use the following curl command to see if you get an expected response. Be sure to replace the IP and password in the command.

```
$ curl -X POST https://[YOUR NORTHBOUND INTERFACE IP HERE]:9443/portalintf -H 'Content-Type: application/json' -k -d '{
    "Vendor": "ruckus",
    "APIVersion": "1.0",
```

```
    "RequestPassword": "YOUR PASSWORD HERE",
    "RequestCategory": "GetConfig",
    "RequestType": "Decrypt",
    "Data": "123456781234",
}'
```

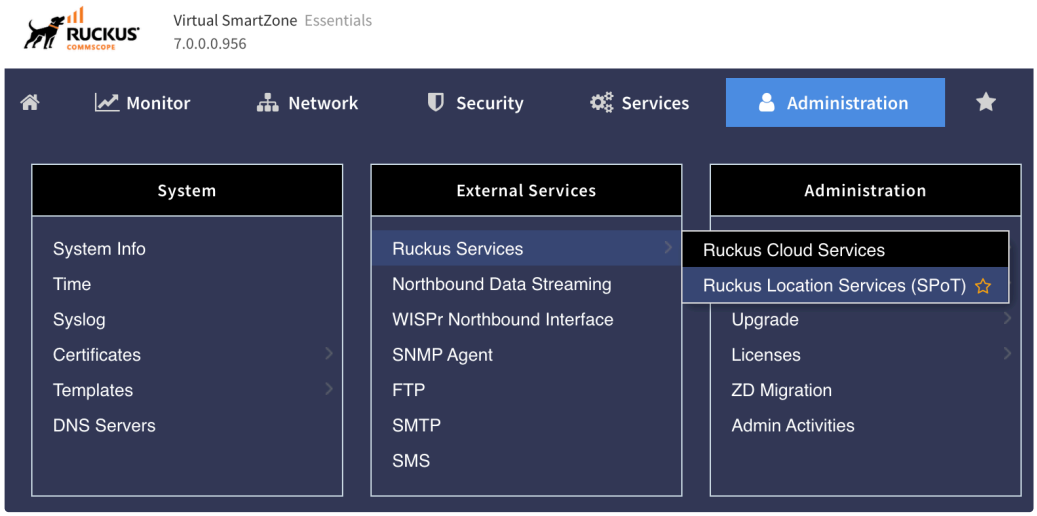
You should see a response like the following:

```
{"ResponseCode":200,"APIVersion":"1.0","Data":"123456781234","Vendor":"Ruckus","ReplyMessage":"OK"}
```

After confirming it works, please share the northbound interface IP and password with your Adentro account manager.

Configure Location Services

1. Select "Administration" > “External Services” > "Ruckus Services" > select “Ruckus Location Services (SPoT)”



2. Choose "Create"
3. Enter the following information:

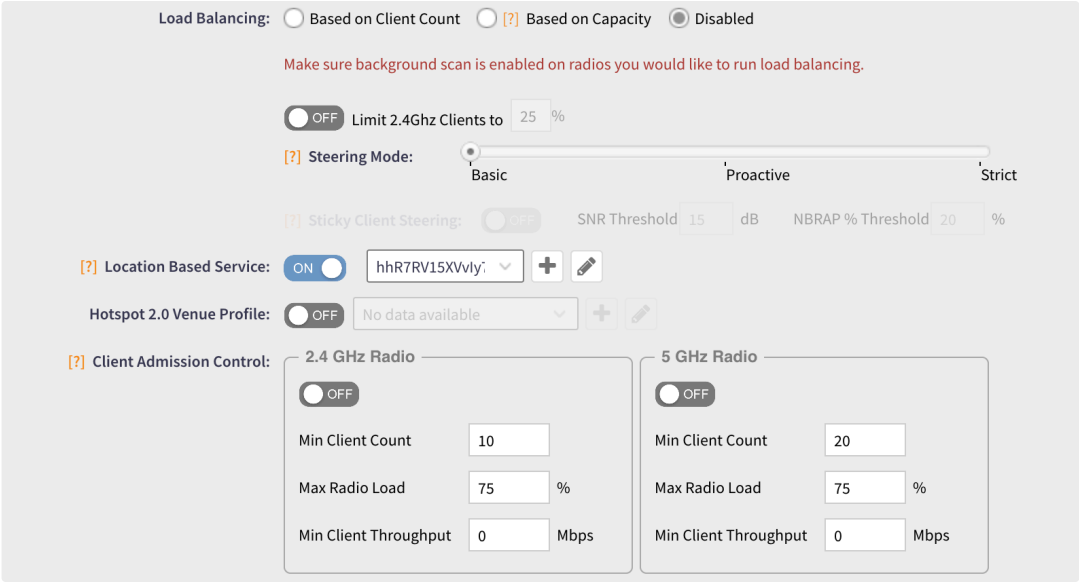
   Venue Name: [Touch base with your Adentro Account Manager to get receive this unique value]

   Server FQDN or IP Address: mqtt.service.zp.cntr.io

   Port: 8883

   Password: [Touch base with your Adentro Account Manager to get receive this unique value]

   TLS Version: tlsv1.2
4. From the main menu, choose “Network” > "Wireless LANs"
5. Edit your guest zone
6. Scroll down to "Advanced Options"
7. Enable "Location Based Service" and select the name of the venue you created in the previous step



You will need to allow traffic on TCP port 8883 for location services to work. Please ensure any firewalls you have are updated to allow this traffic.

Firewall Rules

AAA / RADIUS

TCP/1812, UDP/1813 - Source: SmartZone Controller IP - Destination: RADIUS servers (54.69.8.147 & 54.68.29.80)

WISPr / Guest WiFi

TCP/8099 - Source: Guest Devices (Clients) - Destination: SZ Controller

TCP/9443 - Source: gateway.wifast.com (54.68.113.153, 54.68.53.46, 54.68.126.162) - Destination: SZ Controller

Location Services (MQTT)

TCP/8883 - Source: SmartZone Controller IP - Destination: mqtt.service.zp.cntr.io (34.210.1.57, 44.238.194.89, 44.234.214.75)